CLAIMS

What is claimed is:

1. A method of forming a certificate, comprising:

placing a first public key of a first encryption type in the certificate; and

placing a second public key of a second encryption type in the certificate.

2. The method, as recited in claim 1, wherein the second public key is placed as at least one extension of the certificate.

3. The method, as recited in claim 2, wherein the second encryption type is faster than the first encryption type.

4 The method, as recited in claim 3, wherein the extension where the second public key is placed specifies a key type, a key length, and a key value.

5. The method, as recited in claim 4, wherein the placing of the first public key and the placing of the second public key places the first and second public keys in a certificate information string, where the extension is part of the certificate information string and further comprising:

creating a signature from the certificate information string; and

adding the signature to the certificate information string to form the certificate.

6. The method, as recited in claim 5, further comprising:

placing a hashing algorithm in the certificate information string, wherein the hashing algorithm is used to create the signature; and

placing a certificate authority identifier, which identifies a certificate authority, in the certificate information string.

7. The method, as recited in claim 6, wherein a private key of the certificate authority is used to generate the signature.

8. The method, as recited in claim 1, wherein the placing of the first public key and the placing of the second public key places the first and second public keys in a certificate information string and further comprising:

creating a signature from the certificate information string; and

adding the signature to the certificate information string to form the certificate.

9. The method, as recited in claim 8, further comprising:

placing a hashing algorithm in the certificate information string, wherein the hashing algorithm is used to create the signature; and

placing a certificate authority identifier, which identifies a certificate authority, in the certificate information string, wherein a private key of the certificate authority is used to generate the signature.

10. A method for transmitting a document comprising digitally signing the document, comprising:

encrypting an information string with a private key to create a signature, wherein the private key is related to a public key in a certificate, wherein the certificate comprises a first public key and a second public key, wherein the public key related to the private key is the second public key and wherein the information string contains the document; and

attaching the signature to the information string to create a digitally signed document.

11. The method, as recited in claim 10, wherein the first public key is a first encryption type and the second public key is a second encryption type, which is different from the first encryption type.

12. The method, as recited in claim11, wherein the second encryption type is faster than the first encryption type.

13. The method, as recited in claim 12, wherein the second public key is placed in an extension of the certificate.

14. The method, as recited in claim 13, further comprising adding text to digitally signed document to specify the location of the second public key in the certificate.

15. The method, as recited in claim 14, further comprising hashing the information string, so that the encrypting of the information string encrypts the hashed information string.

16. The method, as recited in claim 15, wherein the extension where the second public key is placed specifies a key type, a key length, and a key value.

17. The method, as recited in claim 16, wherein the certificate further comprises an issuer name, a validity range, and a subject name.

18. The method, as recited in claim 11, further comprising:

transmitting the digitally signed document from a first device; and

receiving the digitally signed document at a second device.

19. The method, as recited in claim 18, wherein the certificate is the certificate for the first device, further comprising:

obtaining the second public key from an extension of the certificate for the first device; and

using the second public key to verify the digitally signed document.

20. The method, as recited in claim 19, further comprising receiving at the second device instructions designating the location of the second public key an the extension of the certificate.